ATTACHMENT B

All property, records, and information, in any format, that constitute fruits, evidence and instrumentalities of violations of 18 United States Code §§ 2252A(a)(2) and (b)(1) (receipt of child pornography), and §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), and attempt and conspiracy to commit those crimes, ("the Target Offenses"), for the time period from April 12, 2019 to present (unless otherwise indicated), including, but not limited, to the following items:

1. Computers, cellular telephones and storage media, as defined below (hereinafter, "device(s)"), used as a means to commit the TARGET OFFENSES;

2. Child pornography, as defined in 18 U.S.C. § 2256(8), and/or visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

3. Any and all information, notes, documents, records, or correspondence, in any format or medium, pertaining to child pornography or sexual activity with or sexual interest in minors;

4. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the digital file(s), or that aid in the identification of persons involved in violations of the TARGET OFFENSES;

5. Records and information relating to the access, viewing or trafficking of child pornography, including correspondence and communications;

6. Records, information, and items relating to the occupancy or ownership of the TARGET PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

7. Records, information, and items relating to control and use of a Burlington Telecom internet subscription, including bills, mail envelopes, and payment information, including checking account, credit or debit card account information;

8. Records, information, and items relating to control and use of IP address 69.5.116.44, including bills, mail envelopes, and payment information, including checking account, credit or debit card account information;

9. For any device whose seizure is otherwise authorized by this warrant:

a. Items 2 to 8 above;

b. Links to child pornography or to online locations where child pornography is stored;

c. Records and information showing access to and/or use of websites and applications used to commit the TARGET OFFENSES;

d. Records of Internet activity related, including logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, and records of internet protocol addresses used;

e. Names, addresses, contact information or lists of names, addresses or contact information, in any format, of those who may have been contacted in connection with the TARGET OFFENSES;

f. Evidence indicating whether and/or when child pornography was accessed and/or viewed by any user of the device;

g. Evidence of who used, accessed, owned, or controlled the device;

h. Evidence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

i. Evidence of the lack of such malicious software;

j. Evidence indicating how and when the device was accessed or used, and evidence indicating the geographic location of the device when it was accessed or used;

k. Evidence of the attachment to the device of other electronic devices or similar containers for electronic evidence;

l. Evidence of counter-forensic programs;

m. Passwords and encryption keys, and other access information that may be necessary to access the device;

n. Evidence of applications used to communicate with other individuals;

o. Evidence of applications used to access and view child pornography and/or visual depictions of minors engaging in sexually explicit conduct;

p. Any and all stored data related to the access, receipt, exchange, or creation of child pornography and/or visual depictions of minors engaging in sexually explicit conduct;

q. Any stored data consisting of evidence of access to child pornography and/or visual depictions of minors engaging in sexually explicit conduct, including Internet logs, Internet browser histories, website bookmarks;

r. Any software used to access hidden-service-websites;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, network hardware, routers and modems, cellular telephones and digital cameras.

The term "storage media" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular telephones capable of storage, floppy

disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

"Child Pornography" is defined in 18 U.S.C. § 2256(8), which includes as any visual depiction of sexually explicit conduct involving the use of a minor; a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct; or a visual depiction that has been created, adapted, or modified to appear than an identifiable minor is engaging in sexually explicit conduct.

"Visual depiction" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

Pursuant to Rule 41(e)(2)(B), it is authorized that electronically stored information may be imaged or copied. Consistent with Rule 41(e)(2)(B), the warrant is deemed executed once the subject computer has been physically seized, and that review of the contents of the subject computer is permitted at a later time.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.